In the modern world of information exchange, there is perhaps none greater a security measure than blockchain technology. With the ability to transfer and receive encrypted data across a decentralized multi-peer network, this phenomenal form of technology can just as easily be used for harm. Aside from industries like cryptocurrency, wherein this technology is highly applicable, blockchain technology is used in industries like that of the healthcare, marketplace, and identity industries, to improve the wellbeing of all parties involved.

The healthcare industry, arguably more than any other industry, involves the transfer of copious amounts of highly confidential data. This exchange of information requires protection from data breaches, and blockchain technology is the absolute best form of security to protect against such breaches. One should consider that , according to Becker's Hospital review, more than 90% of healthcare organizations lose some amount of data to cybercriminals through data breaches. These breaches all too often occur even in the face of cybersecurity measures taken to prevent this. It isn't as much an issue of lax security as it is sophisticated intruders. That said, blockchain technology offers a means of protecting against such breaches, as it cannot be overcome by even the best of hackers. Regulations like HIPAA were implemented for a reason, as sensitive user data is all-too-often all that stands in the way of being allowed to receive certain treatments, or attain and maintain certain positions in an organization. Discriminatory practices can and have been taken against users whose data has been exposed to the public in some way. Blockchain, with its decentralized nature, can easily be used to guard against this. Additionally, healthcare-wsie, the technology can and should be used to improve communication and data-transfer between the numerous organizations that compose the healthcare system, like hospitals, pharmaceutical companies, government health agencies, and the individual. In an industry often plagued by ethical concerns and violations, blockchain offers only an opportunity to solve ethical concerns, and seldom creates them.

Long-gone are the days of marketplaces being confined to small-town markets and county fairs. Today, with the rise of giants like Amazon, much of what is bought and sold is exchanged over the internet, across platforms like Ebay, Craigslist, or Facebook Marketplace. With this exchange comes an age-old issue-scamming. Be it items promised not being sent, or money sent by accident being kept, the exchange of funds across the internet as opposed to in-person has made it extremely difficult to go into the world of online transactions with confidence and an assurance that all will go smoothly. This issue can and , as often as is possible, should be rectified with blockchain. Blockchain in the industry of the marketplace offers the opportunity for producers, sellers, and buyers to interact in trust, confidence, and transparency. Blockchain-based creations like smart contracts allow for secure agreements between all parties involved in any transaction, and should anything go wrong, the immutable nature of data created and exchanged with blockchain technology allows for evidence to be used for or against any party who wishes to indulge in unethical business practices. With blockchain removing the need for intermediaries, marketplace transactions are not only made secure and reliable, but likewise instantaneous. That said, transactions in an already increasingly-fast-paced society (thanks to technology) will become even faster, allowing for a faster advancement of all other industries involved in the marketplace. Although the benefits of blockchain in this industry are many, it also brings with it some concerns. There are certain and (fortunately) unspoken of marketplace-driven industries that deal in the exchange of illegal information, items, or actions. These industries can attribute much of their security and secrecy to technology like blockchain, where it is used for ill on the oft spoken of “dark web”. This can make it extremely difficult for government agencies to source and track illegal activity and pursue perpetrators of heinous crimes committed behind the scenes. It also makes it difficult to attain and develop evidence, either to be used in digging deeper into the organizations of criminals (or the lives of solo criminals) that they come across, or using that evidence in a court of law.

Identity theft is an age-old issue, and though many have fallen victim to the practice over the years, there has perhaps been none a more easier time to steal someone’s identity than in the digital age. With so many platforms in use wherein one must use and promote their identity there exists just as many entry points for cybercriminals. Blockchain technology can remedy this, specifically in how it can address the encryption of the data that composes someone’s identity. Whether one’s identity is stored in the databases of their credit-card company of choice, Bank, favorite social media platform, or local library, data-breaches make it easier for cybercriminals to harvest identities and put it to ill-use through illegal purchases, extortion, and the like. Blockchain technology can allow for user data to be decentralized. Hackers and cybercriminals will find it nearly impossible to access data stores in hospitals, government agencies, and tech companies, which seem to be the most frequent target of cyber-criminals living both domestically and abroad. The identity industry would benefit greatly from needing to, less and less, pursue and investigate cases of identity theft, instead relying on and shifting their practices to more defensive maneuvers like merely reinforcing databases they are tasked with protecting with blockchain technology.

In an age of information, privacy is key, and there are no methods more efficient than blockchain technology when it comes to maintaining data privacy. Across industries like the Healthcare, Marketplace, and Identity industries, decentralized data makes the lives of intruders much more difficult, and develops a certain confidence in the average individual and a willingness to surrender one’s data to organizations like Banks, Hospitals, and government agencies when and where it is needed. However, the robust nature of blockchain technology , since it is merely a tool, makes it just as easy for criminals to use it against government agencies, only increasing the evasive nature of underworld criminal organizations and operations. This is something information scientists must ponder in the days ahead--whether or not data privacy is meant for all, or none at all, for every tool and weapon used for good can be equally useful to those who operate with evil intent. This is the nature of technology.